THE HONORABLE JAMES L. ROBART

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

In Re: Zillow Group, Inc. Session Replay Software Litigation This Documents Refers to: All Actions	Master File No. 2:22-cv-01282-JLR **PLAINTIFFS' OPPOSITION TO MICROSOFT CORPORATION'S MOTION TO DISMISS CONSOLIDATED AMENDED COMPLAINT** **ORAL ARGUMENT REQUESTED**

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

TABLE OF CONTENTS

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

TABLE OF AUTHORITIES

Cases

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Statutes

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Other Authorities

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

I. INTRODUCTION

Plaintiffs Natalie Perkins, Kenneth Hasson, Jamie Huber, David Kauffman, Ashley Popa, Jill Strelzin, Jill Adams, and Jill Adams as natural mother and next friend of her minor child, H.A (collectively "Plaintiffs") brought this class against Zillow Group, Inc. ("Zillow) and Microsoft Corporation ("Microsoft") for their intentional wiretapping of website visitors electronic communications on www.zillow.com. Zillow is a real-estate marketplace company that procured Microsoft as a third-party vendor to embed "Microsoft Clarity," a JavaScript computer code known as "Session Replay Code," on its website. This code is deployed on each website visitor's browser, without consent, to intercept and record every visitor's mouse movements, clicks, scrolls, keystrokes and other electronic communications with the Zillow website in real-time. This practice violates users' privacy and is in violation of wiretap and privacy laws in Washington, Illinois, Pennsylvania, California, and Missouri.

Courts have held that the unbridled use of Session Replay Code to secretly record website visitors' communications is a violation of state wiretapping laws. *See, e.g., Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121 (3d Cir. 2022). Plaintiffs bring these claims on behalf of a nationwide class for (1) violations of the Washington Privacy Act ("WPA"), Wash. Rev. Code §9.73.030 *et seq.*, and (2) for invasion of privacy in violation of Washington common law; alternatively, Plaintiffs also bring claims on behalf of putative state-level classes, for violation of (3) the Pennsylvania Wiretap and Electronic Surveillance Control Act, ("WESCA") 18 Pa. Cons. Stat. 5701, *et seq.*, (4) the California Invasion of Privacy Act ("CIPA"), California Penal Code § 631, (6) the Missouri Wiretap Act ("MWA"), Mo. Ann. Stat. § 542.400, *et seq.* (collectively "State Wiretap Acts"); and the common laws of Illinois, Pennsylvania, and Missouri. Plaintiffs have also sufficiently alleged that Defendants captured their data, communications, and movements using an intercepting device on www.zillow.com and invaded Plaintiffs' seclusion and solitude. Thus, the Court should deny Microsoft's Motion in its entirety. In the alternative, Plaintiffs should be granted leave to amend their Complaint to address any issues concerning the Court.

II. FACTUAL BACKGROUND

The facts of this matter are detailed in Plaintiffs' Consolidated Amended Complaint ("CAC") and are hereby incorporated by reference. In short, this class action is brought against Zillow and its third-party vendor, Microsoft, for the use of Session Replay Code, called Microsoft Clarity, to wiretap the personal and private electronic communications of visitors to Zillow's website. CAC ¶¶ 1, 57. Through this wiretapping, Defendants are able to go beyond understanding user engagement and instead can capture and record nearly every action a website visitor makes immediately, even if the user did not intend to "submit" or "enter" such electronic communications. *Id*. at ¶¶ 34 n. 3, 40–48, 68. Defendants, through the use of Clarity, log *every* interaction a user makes with a website without *any* consent—including, but not limited to, mouse movements and clicks, scrolling, window resizing, user inputs—and then organizes that information into over 30 different categories, including a user's browser, operating system, device, country, and inputted text. *Id*. at ¶¶ 60, 81–82. Clarity can tag a specific user ID to each website visitor to be able to monitor interactions over time to be copied and replayed by Defendants. *Id*. at ¶¶ 60–63. This identifying information will become known and visible to Defendants in order to create "fingerprints that are unique to a particular user's combination of computer and browser settings, screen configuration, and other detectable information." *Id*. at ¶¶ 42, 45.

Each of the named Plaintiffs visited Zillow's website prior to and through 2022. *Id*. ¶¶ 71–79. Plaintiffs regularly visited Zillow's website to browse for homes, search for properties, interact extensively with the website, and enter personal and financial information into text fields during their visits. *Id*. Plaintiffs Perkins, Hasson, Huber, Kauffman, Popa, and Strezlin each entered their names, address, and phone numbers. *Id*. Plaintiffs Perkins, Hasson, Huber, Popa, and Strezlin entered their dates of birth. *Id*. Plaintiffs Perkins, Hasson, and Huber entered their credit score ranges. Plaintiffs Perkins and Huber also entered financial information specifying their current loans and estimates of loans. These are all considered personally identifiable information that was subject to unlawful monitoring, recording, and collection by Microsoft Clarity. *Id*. at ¶ 81. Ultimately, Defendants' secret deployment of Clarity results in the electronic equivalent of

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

"looking over the shoulder" of each visitor to Zillow's website for the entire duration of their website interaction. *Id.* ¶ 2. Defendants' wiretapping with their Session Replay Code is ongoing and continues to present legitimate harm to website visitors in exchange for their own profit. *Id.* ¶¶ 24, 26, 87. Zillow and Microsoft thereby violated the aforementioned wiretapping statutes and common laws, and their conduct constitutes an invasion of the privacy rights of the Plaintiffs and Class Members.

III. ARGUMENT

A. PLAINTIFFS AND THE CLASS MEMBERS COMMUNICATED WITH ZILLOW

Microsoft asserts that it cannot be liable under the State Wiretap Acts because Plaintiffs' substantive interactions with Zillow's website were not "communications." Mot. at 8–10. This position is untenable and contradictory to the facts alleged in Plaintiffs' Amended Complaint. While Microsoft asks this Court to part and parcel the definition of "communication" outside of the context in which the word is used in the Acts, it cannot escape that Plaintiffs clearly allege these were communications, and courts are nearly uniform in treating them as such. CAC at ¶¶ 2, 4, 47, 63–65, 79–81, 85, 89, 93, 95.

The case law cited by Microsoft in support of its position relies on conflating "communications" with "content." In support of its argument that mouse clicks and movements are not communications, Microsoft cites to *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1082–83 (C.D. Cal. 2021), which states "[n]one of these pieces of data constitutes message ***content.***" (emphasis added). In fact, the court in that case did not address whether the plaintiff's interactions with the website were communications, making the case entirely irrelevant to Microsoft's argument here.

Microsoft's citations to Florida decisions in *Jacome v. Spirit Airlines Inc.*, No. 2021-000947-CA-01, 2021 WL 3087860, at *4 (Fla. Cir. Ct. June 17, 2021) and *Goldstein v. Costco Wholesale Corp.*, 559 F. Supp. 3d 1318, 1319, 1321–22 (S.D. Fla. 2021) belie Microsoft's argument. Both the Federal Wiretap Act, 18 U.S.C. § 2510 *et seq* ("FWA") and the Florida Security of Communications Act explicitly exclude communications from tracking devices from

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

the definitions of communications. *Jacome*, 2021 WL 3087860 at *3. Such an explicit exclusion would not be necessary, or even reasonable, if the very actions specifically excluded from the definition of "communications" were not, in fact, communications.

Microsoft asserts that the decisions in *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503 (C.D. Cal. 2021) and *Revitch v. New Moosejaw, LLC*, No. 18-CV-06827-VC, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2021) are "unpersuasive and unhelpful" because the court "failed to analyze whether browsing a website equals communicating with it." *Id*. at 10 n.6. However, the fact that Microsoft's position is contradicted by the court's clear mandate does not equate to failure to analyze on the part of the court. *See Revitch*, 2019 WL 5485330, at *1 ("Revitch's interactions with the Moosejaw website is communication within the meaning of section 631.")[1]

Microsoft asks this Court to dismiss Plaintiffs' claims on the basis of Microsoft's own confusion between "what is a communication" versus "what are the contents of a communication." Plaintiffs' respectfully request this Court decline to do so, as the CAC contains well pleaded allegations that support that the data intercepted by Defendants included "something . . . communicated to someone," including "visitor's personal and private sensitive data" such as "medical conditions, credit card details, and other personal information displayed or entered on webpages." *State v. Ozuna*, 359 P.3d 739, 744 (Wash. 2015); CAC ¶¶ 2, 33, 34, 39, 42–44, 46, 47, 50–51, 60, 63, 71–79, 82, 84, 89–91, 95.

B. PLAINTIFFS SUFFICIENTLY ALLEGED MICROSOFT VIOLATED THE WASHINGTON PRIVACY ACT

Plaintiffs assert Microsoft violated the WPA by capturing and recording Plaintiffs' private Web Communications with Zillow. CAC ¶¶ 116–27. Under the WPA, it is "unlawful for any individual, partnership, corporation, association . . . to intercept, or record any . . . [p]rivate communication transmitted by . . . device between two or more individuals . . . without first obtaining the consent of all the participants in the communication." RCW § 9.73.030(1)(a).

[1] Admittedly, the court in *Saleh* did not discuss whether or not the plaintiff's interactions with the defendant's website were communications; however, it appears that the Court and both parties in that case do not question whether such interactions to be communications under CIPA, as that issue was not raised.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

The WPA is one of the strictest wiretapping statutes in the nation. *State v. Kipp*, 317 P.3d 1029, 1031 (Wash. 2014) ("Washington State's privacy act is considered one of the most restrictive in the nation."). "Washington has a long history of extending strong protections to telephone and other electronic communications" and the WPA is "broad, detailed and extends considerably greater protection to [its] citizens in this regard than do comparable federal statutes and rulings thereon." *State v. Gunwall*, 720 P.2d 808, 815 (Wash. 1986). Washington, likewise, has recognized the need to "interpret the privacy act in a manner that ensures that the private conversations of this state's residents are protected in the face of an ever-changing technological landscape." *State v. Christensen*, 102 P.3d 789, 794 (Wash. 2004) ("We must interpret the privacy act in a manner that ensures that the private conversations of this state's residents are protected in the face of an ever-changing technological landscape."). This case involves the "ever-changing" technological landscape, specifically, session replay technology that records users' every interaction, communication, and movement performed on a webpage.

Here, Plaintiffs allege Microsoft violated the WPA by installing its session replay technology, Clarity, on Plaintiffs' browsers upon connecting to Zillow's website. CAC ¶ 35. Clarity proceeded to capture and record all of Plaintiffs' interactions with Zillow's website, including personal information Plaintiffs typed into Zillow about themselves, and which Microsoft could use to create user IDs to further their tracking of Plaintiffs' information. *Id.* at ¶¶ 36, 38–46. Clarity's interception and recording occurred without Plaintiffs' knowledge and caused them both economic and emotional harm. CAC ¶¶ 96–99, 138–40.

Despite this, Microsoft deploys a number of semantic arguments seeking to escape liability. Specifically, Microsoft contends that: (1) the WPA supposedly only covers communications between "human being[s]"; (2) the communications were not "private" because Plaintiffs allegedly consented to the use of session replay technology through a Privacy Policy hidden at the bottom of Zillow's webpage; (3) the communications were not "intercepted"; and (4) Clarity is not a "device" under the WPA. Microsoft also asks the Court to disregard Plaintiffs' alleged injuries and find its wiretapping software caused no harm. The Court should reject these arguments.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

1. The WPA Protects Plaintiffs' Web Communications with Zillow

Microsoft contends that the WPA does not apply here because the Web communications at issue were not between two people. Mot. at 11 (citing RCW § 9.73.030(1) (prohibiting interception or recording of communications between "two or more individuals"). Microsoft has raised a similar argument before, and it was rejected. In *Russo v. Microsoft Corp.*, No. 4:20-cv-4818, 2021 WL 2688850 (N.D. Cal. June 30, 2021), the court rejected Microsoft's claim that the WPA does not apply to corporations. *Id.* at *7 ("Under Microsoft's interpretation, the Washington Legislature created liability against a broad range of entities, but only provided a cause of action against individuals, which is implausible" and recognizing that the use of "person" includes corporations). *Russo* held that, contrary to Microsoft's claims, the term "person" under the WPA includes both individuals and, among other things, corporate entities. *Id.*

Microsoft argues that the WPA's use of the term "individuals" is meant to mean only "human beings," and, thus, would not include communications with a corporation like Zillow. Mot. at 11. A company like Zillow, however, is merely an "association with another" or "a group of persons." *Company*, Merriam-Webster.com (last visited, July 31, 2023), https://www.merriam-webster.com/dictionary/company. The WPA would apply equally to communications between a group of persons, assuming they were intended to be private, as it would to an individual. *See, e.g.*, RCW § 9.73.030(1)(a) (protecting communications "between two *or more* people." (emphasis added)).

Moreover, other courts analyzing less conservative wiretap statutes have recognized that web browser interactions are communications. *See, e.g., In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 607 (9th Cir. 2020) (treating transmissions between a user and webpage as communications); *see also In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 934 F.3d 316, 325 (3rd Cir. 2019) ("In an era when millions of Americans conduct their affairs increasingly through electronic devices, the assertion . . . that federal courts are powerless to provide a remedy when an internet company surreptitiously collects private data . . . is untenable.").

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Microsoft cites no authority to the contrary. Rather, its cases involve no communications at all. For instance, in *Cousineau v. Microsoft Corp.*, 992 F. Supp. 2d 1116, 1129 (W.D. Wash. 2012), the court dismissed a WPA claim where plaintiff's phone stored its geo-location, which was allegedly accessible by Microsoft. *Id.* at 1119. However, as the court noted, the only two parties at issue were the plaintiff and Microsoft, and if Microsoft intercepted the communication, the plaintiff needed to identify another party to whom she was communicating for the WPA to apply. *See id*. The court never held, as Microsoft claims, that her communication were not protected by the WPA because Microsoft was not an "individual." Thus, the Court should reject Microsoft's claim that the WPA does not protect communications with companies.

2. Plaintiffs' Communications with Zillow were Private

Microsoft also asserts that Plaintiffs' communications with Zillow were not private because unbeknownst to Plaintiffs, Zillow had placed a Privacy Policy at the bottom of its webpage supposedly disclosing its use of session replay technology. Mot. at 12. Where, as here, a reasonable person would not be aware of the Privacy Policy, they cannot be deemed to have consented to it. *Savetsky v. Pre-Paid Legal Servs., Inc.*, No. 14-cv-3514, 2015 WL 605767, at *3 (N.D. Cal. Feb. 12, 2015) (describing "browsewrap" agreements where a website "contains a notice that—by using the services of, obtaining information from, or initiating applications within the website—the user is agreeing to and is bound by the site's terms" and that "courts generally require users have actual or constructive knowledge of a website's terms and conditions before enforcing browsewrap agreements."); *Nguyen v. Barnes & Noble, Inc.*, 763 F.3d 1171, 1176 (9th Cir. 2014) (finding terms of a browsewrap agreement unenforceable); *see also McGhee v. N. Am. Bancard, LLC*, 755 F. App'x 718, 720 (9th Cir. 2019) ("The onus fell on the [defendant] to put its customers on notice of the binding terms of the contract in a clear and straightforward way.").

Plaintiffs, here, specifically allege that they did not consent to the use of Session Replay Code by Zillow and Microsoft, did not view Zillow's Privacy Policy, and had no awareness of either the policy or Zillow's use of Clarity. CAC ¶ 98. Plaintiffs reasonably believed that their interactions with Zillow's website would remain between them, and that Zillow had not invited an

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

unknown third-party to surreptitiously obtain and record those communications. *See id.* at ¶ 28. The Court should find Plaintiffs' communications were private.[2]

3. Clarity Intercepted Plaintiffs' Communications with Zillow

Plaintiffs pled that Microsoft's Clarity works by duplicating communications instantaneously at the point of their transmission. CAC ¶ 85. Despite that, Microsoft argues that Clarity did not "intercept" communications supposedly because it did not obtain the communications prior to receipt by Zillow. That contention fails for two reasons—the WPA also prohibits recording communications, as Microsoft did here, and Microsoft's claim disregards Plaintiffs' allegations, which plainly describe Clarity as having intercepted communications prior to receipt by Zillow.

First, the WPA is not limited solely to the interception of communications; it also encompasses the recording of communications. RCW § 9.73.030(1) ("[I]t shall be unlawful . . . to intercept, ***or record*** any . . . private communication . . . ." (emphasis added)). Plaintiffs alleged that Clarity recorded their communications with Zillow and, thus, they violated the WPA regardless of interception. *State v. Novick*, 384 P.3d 252, 257 (Wash. Ct. App. 2016) (holding that "RC 9.73.030 prohibits recording conversations without the consent of each participant in that conversation" and upholding conviction under 9.73.030 for using a computer program to automatically record victim's communications).

Second, Plaintiffs also adequately alleged Zillow intercepted their communications. The Washington Supreme Court held that the term "intercept" should "be given [its] ordinary meaning" to "stop, . . . or interrupt in progress or course before arrival." *State v. Roden*, 321 P.3d 1183, 1188 (Wash. 2014). That is exactly what Clarity does—intercepts the communication upon transmission and before receipt by Zillow. Plaintiffs pled that Clarity "intercepts the contents of the[]

[2] Microsoft cites *State v. Corliss*, 838 P.2d 1149 (Wash. Ct. App. 1992), and claims that a telephone conversation was not "private" because of the risk "someone else . . . [could] listen." Mot. at 12. The Washington Supreme Court, on appeal, did not adopt that holding. *State v. Corliss*, 870 P.2d 317, 320 (Wash. 1994) (holding "no violation of the statute [occurred] because the conversation was not 'intercepted' by a 'device'" and stating "[o]ur holding goes no further."). Washington courts have also "repeatedly held that the mere possibility that intrusion on otherwise private activities is technologically feasible does not strip citizens of their privacy rights." *Christensen*, 102 P.3d at 792.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

communications ***between*** Plaintiffs and Zillow." CAC, ¶ 85 (emphasis added). Plaintiffs further explained that, through Clarity, "electronic communications are intercepted contemporaneously with their transmission," meaning that the communications are intercepted at the time they are first made. *Id.* at ¶ 24. Thus, Clarity did exactly what Microsoft claims is required—intercepted the communications "before arrival."

Moreover, if Microsoft's claim that interception requires "stopping" or "preventing" a communication from arriving, then the quintessential medium that the WPA was enacted to protect—telephone conversations—would be unprotected because an interception does not slow down the progress of the communication. *See, e.g.*, *State v. Hinton*, 319 P.3d 9, 14 (Wash. 2014) (noting "Washington's long history of extending strong protections to telephonic and other electronic communications" and that "intercepting or recording telephone class violates the privacy except under narrow circumstances."). Such a result is unsupported by case law or purpose of the WPA. The Court should hold Clarity intercepted Plaintiffs' communications.

4. Clarity is a Device Under the WPA

The Court should also find that Clarity is a "device" under the WPA. While the WPA does not define "device," software that intercepts and records communications are actionable under the WPA. In *Novick*, the Washington Court of Appeals upheld a conviction for, among other things, violating the WPA where the defendant used a program called "Mobile Spy" to capture a victim's text messages, call logs, and e-mails. 384 P.3d at 259. Clarity works much the same way, using software to reconfigure users' browsers to redirect communications intended for Zillow to Microsoft. CAC ¶¶ 92–94. Consequently, Clarity is a "device" under the WPA.

5. Plaintiffs Did Not Consent to the Acquisition of Their Data

Microsoft's argument that Plaintiffs consented to the acquisition of their data is merely a rehashing of its argument that Plaintiffs' communications with Zillow's website were not "private." Mot. at 11–13. The fact that a person is deemed to have consented to the recording of email and text messages under WPA has no bearing on this case.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

6. Plaintiffs Adequately Alleged an Injury under the WPA

Finally, Plaintiffs have adequately pled an injury. The WPA permits recovery for a broad range of injuries including harm to "his or her business, his or person, or his or her reputation" and "actual damages," "mental pain and suffering," or "liquidated damages." RCW § 9.73.060. While Washington state courts have not analyzed precisely what constitutes an injury under the WPA, they have analyzed similar statutes and found the types of actionable injuries to be broad.

For example, the Washington Consumer Protection Act ("WCPA") permits recovery for "an injury to the claimant's business or property," a more restrictive requirement than the WPA. *Sign-O-Lite Signs, Inc. v. DeLaurenti Florists, Inc.*, 825 P.2d 714, 720 (Wash. Ct. App. 1992). Even so, courts have held that the injury "need not be great" and that "with respect to injury, . . . 'no monetary damages need be proven'" and even "'nonquantifiable injuries . . . would suffice for the [injury] element of the [WCPA.]'" *Id.* at 720 (quoting *Nordstrom, Inc. v. Tampourlos*, 733 P.2d 208, 211 (Wash. 1987)); *St. Paul Fire & Marine Ins. Co. v. Updegrave*, 656 P.2d 1130, 1133 (Wash. Ct. App. 1983) ("The consumer need not show specific monetary damages to recover under the Act."); *Sign-O-Lite*, 825 P.2d at 720 (requiring only "some evidence, however slight, to show an injury to the claimants' business or property.").

Like the WCPA's injury requirement, the WPA requires only a minimal injury, especially given the WPA's overwhelming interest in protecting private communications. *See, e.g., State v. Christensen*, 102 P.3d 789, 794 (Wash. 2004); *Lewis v. State Dep't of Licensing*, 139 P.3d 1078, 1082 (Wash. 2006); *Kipp*, 317 P.3d at 1031. Here, Plaintiffs pled both mental and emotional suffering and economic loss. CAC ¶ 138 ("Defendants' conduct has caused Plaintiffs . . . mental anguish and suffering arising from their loss of privacy and confidentiality of their electronic communications."); *Id.* ¶ 139 ("This disclosure and loss of privacy and confidentiality has caused Plaintiffs . . . to experience mental anguish, emotional distress, worry, fear, and other harms."); *Id.* ¶ 140 ("Defendants deprived Plaintiffs . . . of the economic value of their interactions with Zillow's website."). These type of harms are recoverable under the WPA. RCW § 9.73.060 (permitting recovery for "mental pain and suffering."); *Panag v. Farmers Ins. Co. of Washington*, 166 Wn.2d

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

27, 57 (Wash. 2009) (holding, under the WCPA's similar injury component, that "the injury requirement is met upon proof the plaintiff's property interest or money is diminished because of the unlawful conduct even if the expenses caused by the statutory violation are minimal."). Consequently, Plaintiffs have pled an adequate injury.

C. DEFENDANT OVERSTATES THE "AURAL" REQUIREMENT FOR PLAINTIFFS' MISSOURI WIRETAPPING CLAIMS.

Defendant first attempts to dismiss Plaintiffs' Missouri wiretapping claim by imposing an aural condition on the communications at issue. The MWA is, as Defendant admits, mostly modeled after the FWA. Mot. at 18. In that vein, it must be construed as at least as protective of the privacy interests at issue as the federal statute. In considering a state wiretapping statute, the Third Circuit held:

> [Pennsylvania's Wiretapping and Electronic Surveillance Control Act] prohibits intercepting communications while allowing someone whose communications have been intercepted to sue the offender. It also operates in conjunction with and as a supplement to the Federal Wiretap Act, 18 U.S.C. § 2510 *et seq.*, which provides uniform minimum protections for wire, electronic, or oral communications. The States—like Pennsylvania—may "grant greater, but not lesser, protection than that available under federal law," as the WESCA does.

Popa, 52 F.4th at 125–26 (quoting *Commonwealth v. Spangler*, 570 Pa. 226, 809 A.2d 234, 237 (2002)). The FWA, as amended by the Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 ("ECPA"), does not have an audible requirement; a restriction requiring an audible communication would be a lesser protection of the regulated conduct. Defendant states that the FWA requires capture of "audible data," but this is incorrect. *See, e.g.*, *United States v. Szymuszkiewicz*, 622 F.3d 701, 705 (7th Cir. 2010) (finding application of the FWA for interception of email); 18 U.S.C.A. § 2510 (4) (defining "intercept" as "the aural **or** other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.") (emphasis added).

Microsoft asserts that Adams has not pleaded a proper claim for interception because there is no "aural acquisition" at issue. Mot. at 17. But at least one Missouri court has applied the concept

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

of "wire communications" to include non-spoken communications, such as email. *Phillips v. Am. Motorist Ins. Co.*, 996 S.W.2d 584, 591 (Mo. Ct. App. 1999). Microsoft's narrow reading of the MWA is unwarranted.

Microsoft next asserts that Adams has not alleged the use of a "device." Mot. at 17. Many courts have accepted that computer code can constitute a "device" for the purposes of a claim under the FWA. The Wiretap Act broadly prohibits the use of "any device or apparatus which can be used to intercept a wire, oral, or electronic communication." 18 U.S.C. § 2510(5).[3] Courts have found similar spyware or third-party cookies, including code known as a "tracking pixel," to be such a device. *See, e.g., In re Meta Pixel Healthcare Litig.*, No. 22-CV-03580-WHO, 2022 WL 17869218, at *12 (N.D. Cal. Dec. 22, 2022). Courts routinely find that software designed to record and transmit internet communications are "devices" under § 2510(5). *United States v. Hutchins*, 361 F. Supp. 3d 779, 795 (E.D. Wis. 2019) ("Section 2510(5)'s reference to 'mechanism,' which is commonly defined as a 'process, technique, or system for achieving a result' seems to encompass software."); *Luis v. Zang*, 833 F.3d 619, 634 (6th Cir. 2016) ("WebWatcher is a device specifically designed to surreptitiously "intercept[ ] communications"); *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1084 (N.D. Cal. 2015) ("Plaintiffs have sufficiently alleged that the Carrier IQ Software is a 'device' for purposes of the Wiretap Act."); *Klumb v. Goan*, 884 F. Supp. 2d 644, 661 (E.D. Tenn. 2012) (spyware software). Accordingly, Microsoft's bald assertion that Plaintiffs have failed to allege the use of a 'device' is without merit.

Microsoft attempts to draw a distinction between the ECPA, which clearly applies to all electronic communications, and the MWA, which it contends does not. Mot. at 18 ("that term [interception] applies only to communications via common carrier telephone services.")

[3] *See also, e.g., United States v. Mitra*, 405 F.3d 492, 495 (7th Cir. 2005) (acknowledging that general technology statute should be read broadly in order to accommodate new developments). It should be noted that the cases Microsoft cites regarding "devices" under Missouri law are from 1998. Since then, tracking and spying technology has grown more sophisticated, and there is no reason to believe Missouri law would not be construed to keep pace.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Microsoft's argument amounts to the reductive assertion that without a wire, there can be no wiretapping. Defendant cites to no contemporary cases where a court in Missouri has held as such.

Missouri law regarding wiretapping makes only one reference to cellular phone technology, in Mo. Stat. § 542.408.4(2). In this single instance, however, the clear intent of the statute is to conflate wireless cellular phones with a "wire communication." Defendant's interpretation would lead to the absurd conclusion that the determination of whether an internet communication interception was wrongful would depend upon whether a person on the internet was using a wireless modem or a dial-up telephone line-based modem, because the latter would include a wire and the former acts over the air. There is no reason to adopt such a reductive or Manichean approach.

In interpreting the FWA, courts have acknowledged the ongoing evolution of technology and the corresponding need for the law to evolve with it as well. Under the FWA, courts have found that "simultaneous, unknown duplication and communication of GET requests do not exempt a defendant from liability under the party exception." *In re Facebook*, 956 F.3d at 608. As the Ninth Circuit noted in examining the party exception of the FWA:

> [w]e also recognize that the Wiretap Act's legislative history evidences Congress's intent to prevent the acquisition of the contents of a message by an unauthorized third-party or 'an unseen auditor.' Permitting an entity to engage in the unauthorized duplication and forwarding of unknowing users' information would render permissible the most common methods of intrusion, allowing the exception to swallow the rule.

Id. (citing to S. REP. NO. 90-1097, *reprinted in* 1986 U.S.C.C.A.N. 2112, 2154, 2182). There is no reason to believe that Missouri, having modeled its statute on the FWA, would permit "listening in" on communications merely because the technology was more advanced than a landline telephone.

Finally, Microsoft attempts to take refuge in the consent of Zillow, a party to the communications at issue. Microsoft mistakenly suggests that the alleged tortious or criminal acts, which would negate the consent exception, must exclusively involve violations of the MWA and

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

invasion of privacy claims. However, no such specific requirement exists. Adams has also alleged violations of the MMPA. CAC ¶¶ 241–62. This is also a criminal statute. *See* Mo. Stat. § 407.020.3. The alleged violation of the MMPA involves the failure to disclose the surreptitious eavesdropping, and not, as Microsoft asserts, the recording itself. A violation of the MMPA, as well as the allegations of invasion of privacy, is enough to satisfy the crime-tort exception.

D. PLAINTIFFS SUFFICIENTLY PLEADED A CLAIM FOR A VIOLATION OF CIPA.

1. Microsoft's Liability Under CIPA is Premised Upon Willfully Attempting to Learn the Contents or Meaning of a Communication in Transit Under Prong 2, not Intentional Wiretapping Under Prong 1.

Microsoft argues that Plaintiffs' CIPA claim fails because they have not alleged an interception involving telephone or telegraph equipment. However, Plaintiffs' CIPA claims are not based on the first prong of Section 631(a), but rather the second prong which makes liable anyone who "reads, or attempts to read, or to learn the contents" of a communication "without the consent of all parties to the communication." Cal. Penal Code § 631(a). Courts have concluded that the second prong of Section 631(a) applies when a defendant attempts to eavesdrop on electronic communications that occur over the internet. *See Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022); *Yoon*, 549 F. Supp. 3d at 1080; *Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (collecting cases).

2. Microsoft Intercepted the "Contents" of Plaintiffs' Electronic Communications.

Microsoft incorrectly argues that it did not intercept the "contents or meaning of any message, report, or communication" because Plaintiffs did not communicate with Zillow. Mot. at 21–22. "The analysis for a violation of [CIPA] . . . is the same as that under the federal Wiretap Act [18 U.S.C. §§ 2510–2523, the Electronic Communications Privacy Act of 1986]" (the "[Federal] Wiretap Act"). *Saleh*, 562 F. Supp. 3d at 517 (quoting *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020)). The FWA broadly defines "contents" as "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8). The

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Ninth Circuit has interpreted "contents" under the FWA to refer to the intended message conveyed by the communication but not record information regarding the characteristics of the message that is generated in the course of the communication. *Graf v. Zynga Game Network, Inc. (In re Zynga Privacy Litig.)*, 750 F.3d 1098, 1107 (9th Cir. 2014). However, "[w]hether information is 'content" or 'record information' can depend in part on the manner in which the information is generated, as information that would otherwise be considered 'record information'—such as names, addresses, telephone numbers, and email addresses—may be 'contents' of a communication where the user communicates with a website by entering his information into a form provided by the website." *Saleh*, 562 F. Supp. 3d at 517 (citing *In re Zynga*, 750 F.3d at 1107).

Applying this definition of "contents," the *Saleh* Court addressed the same issue Microsoft now raises in a nearly identical case. Specifically, in *Saleh*, the plaintiff brought CIPA claims against Nike and FullStory for utilizing Session Replay Code to capture their "mouse movements, clicks, typing, scrolling, swiping, tapping, keystrokes, geographic location, IP addresses, and data entry" on Nike's website. The defendants argued that this information was not "contents" under CIPA. *Id.* at 517–18. The *Saleh* Court recognized that some portion of this information was properly considered "contents," ultimately concluding that the "Plaintiff [ ] met his burden to allege facts plausibly showing Defendants recorded Plaintiff's content communications with Nike by recording, among other things, keystrokes and a video of Plaintiff's interactions with Nike's website." *Id.* at 518; *see also Byars v. Goodyear Tire & Rubber Co.*, No. 522CV01358SSSKKX, 2023 WL 1788553, at *4 (C.D. Cal. Feb. 3, 2023) (following *Saleh* and concluding that the interception of chat communications with a website were "content").[4]

Like *Saleh*, Plaintiffs allege that Microsoft Clarity intercepted their Website Communications in real time, including their mouse movements, clicks, keystrokes, URLs of webpages visited, and more, and that this information was used by Microsoft to recreate and replay

[4] In reaching this conclusion, the *Saleh* Court rejected the defendants' reliance on *Goldstein*, 559 F. Supp. 3d at 1321, which interpreted "contents" under the Florida Security of Communications Act ("FSCA") because *Goldstein* turned on an FSCA exemption that does not exist under CIPA. *See Saleh*, 562 F. Supp. 3d at 518. The Court should therefore follow *Saleh* and reject Microsoft's attempt to rely on *Goldstein* and *Jacome*.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

their entire interaction with www.zillow.com. CAC ¶¶ 1, 60–61, 63. Plaintiffs also allege that Microsoft captured detailed information about their browsing habits for homes for sale along with personal information, including names, addresses, and phone numbers, along with information about properties owned and information required to submit offers to purchase properties. CAC ¶¶ 74, 83–84. This is exactly the type of substantive information that Courts consider "content" as opposed to "record information." *See Katz-Lacabe v. Oracle Am., Inc.*, No. 22-CV-04792-RS, 2023 WL 2838118, at *9 (N.D. Cal. Apr. 6, 2023) (finding that personal information such as names, dates of birth, and medical information entered to form fields was "content").

Microsoft attempts to escape liability by arguing that even if Plaintiffs' intercepted Website Communications are communicative, Plaintiffs' CIPA claim fails because Microsoft Clarity "masked" any sensitive text collected. Mot. at 24. This argument fails for two reasons. First, there is no requirement that Plaintiffs must allege the exact contents of their communications with Zillow that were intercepted at this stage. Plaintiffs must merely allege non-record information has been intercepted, which they have. *See Saleh*, 562 F. Supp. 3d at 517–518. Second, at the motion to dismiss stage, all well-pleaded facts and inferences are to be drawn in Plaintiffs' favor. *See Wilson v. Hewlett–Packard Co.*, 668 F.3d 1136, 1140 (9th Cir. 2012) (explaining that when evaluating a complaint under Rule 12(b)(6), the court "must accept all well-pleaded material facts as true and draw all reasonable inferences in favor of the plaintiff."). The use and effectiveness of Microsoft Clarity's "masking" is an issue of fact that cannot be decided at this juncture. *See* Mot. at 13 ("unless Zillow affirmatively *changed* the masking setting.") (emphasis in original).

3. Plaintiffs' Electronic Communications were Intercepted in Transit

Microsoft argues that Plaintiffs' CIPA claim fails because they have not alleged any electronic communications were intercepted "in transit." Such an argument ignores the well-pleaded facts of the CAC. Courts have explained that the interception of electronic communications occurs "in transit" under CIPA when they are acquired during transmission. *Hazel v. Prudential Fin., Inc.*, No. 22-CV-07465-CRB, 2023 WL 3933073, at *2 (N.D. Cal. June 9, 2023)

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

(collecting cases). Here, Plaintiffs have alleged that Microsoft Clarity intercepted their Website Communications in "real time." CAC ¶¶ 61, 81. Plaintiffs further allege the wiretapping by Microsoft Clarity was ongoing for the duration of their visits to www.zillow.com and began immediately upon arriving on the website. CAC ¶¶ 85, 96. Finally, Microsoft Clarity's instantaneous interception of Website Communications is demonstrated by the mere 30 milliseconds it takes for Microsoft Clarity to send the captured Website Communications to Microsoft. CAC ¶ 85. These allegations are sufficient to allege that the interception occurred "in transit" at the motion to dismiss stage. *See Hazel*, 2023 WL 3933073, at *3; *see also Luis*, 833 F.3d at 629–31.

4. Microsoft Acted "Willfully"

Microsoft argues that it cannot be liable for a violation of CIPA because it did not "willfully" engage in a violation of CIPA. Microsoft's argument fails. The word "willfully," when applied to the intent requirement under the California Penal Code, such as Cal. Penal Code § 631(a), "implies simply a purpose or willingness to commit the act, or make the omission referred to. It does not require any intent to violate law, or to injure another, or to acquire any advantage." Cal. Penal Code § 7(a); *see also People v. Lewis*, 15 Cal. Rptr. 3d 891, 901 (Cal. App. 2004) ("The word 'willfully' as generally used in the law is a synonym for 'intentionally,' i.e., the defendant intended to do the act proscribed by the penal statute."). In the wiretapping context, a defendant acts willfully, *i.e.*, intentionally, when it designs software for the purpose of surreptitiously intercepting electronic communications and the defendant receives such electronic communications through the very software it designed. *See In re Meta Pixel*, 2022 WL 17869218, at *11; *Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 684 (N.D. Cal. 2021) (defendant intentionally intercepted communications when it knew its software was intercepting private communications but failed to take remedial action).

Here, Plaintiffs allege that Microsoft designed Microsoft Clarity for the purpose of secretly collecting, monitoring, and recording individuals' Website Communications in real time to

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

recreate and replay a visitor's entire interaction with a website such as www.zillow.com. CAC ¶¶ 57, 60–61, 63. Further, Microsoft Clarity operates in the background of a webpage, and can be revealed only by certain web technologies such as "developer tools." CAC ¶ 67. Finally, Plaintiffs allege that Microsoft receives the Website Communications intercepted by Microsoft Clarity. CAC ¶¶ 69, 81, 83. It is wholly irrelevant that Microsoft has no control over Zillow's website or the activities of Zillow website users. Microsoft designed wiretapping software and received Website Communications as a result of supplying that software to companies such as Zillow. For these reasons, Plaintiffs have sufficiently alleged that Microsoft "willfully and without the consent of all parties to the communication, . . . read[ ], or attempt[ed] to read, or [ ] learn[ed] the contents or meaning of any message, report, or communication."

E. DEFENDANT CANNOT AVOID LIABILITY BY ASSERTING THE MISAPPLICATION OF THE RULE OF LENITY

Microsoft's reliance on the rule of lenity is simply inappropriate in this action. While Defendant cites to a number of terms it deems to be ambiguous, seemingly on the sole basis that the terms are not expressly defined by the statutes, "the rule of lenity is not applicable unless there is a ***grievous*** ambiguity or uncertainty in the language and structure of the statute, such that even after a court has seized every thing from which aid can be derived, it is still left with an ambiguous statute." *Chapman v. United States*, 500 U.S. 453, 455, 111 S. Ct. 1919, 1922 (1991) (emphasis added) (internal quotations omitted); *see also United States v. Hall*, 972 F.2d 67, 69 (4th Cir. 1992) (same); *United States v. Crowell*, 9 F.3d 1452, 1452 (9th Cir. 1993) ("The rule of lenity comes into operation at the end of the process of construing what congress has expressed, not at the beginning as an overriding consideration of being lenient to wrongdoers").

Plaintiffs have clearly alleged the invasion of their rights to privacy, and the purpose of wiretapping statutes at all levels is without question; to protect the privacy of communications and information from interception. *See Davis v. Facebook, Inc.*, 956 F.3d 589, 598 (9th Cir. 2020) (collecting cases and noting that "the legislative history and statutory text demonstrate that

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Congress and the California legislature intended to protect [] historical privacy rights when they passed the Wiretap Act, SCA, and CIPA . . . [The Wiretap Act] is the primary law protecting the security and privacy of business and personal communications in the United States today.. . . [The SCA] is modeled after the Right to Financial Privacy Act, 12 U.S.C. § 3401 *et seq*. to protect privacy interests in personal and proprietary information.. . . CIPA was passed to protect the right of privacy of the people of this state.'") (internal quotations omitted). Defendant's manufactured uncertainties hardly rise to the standard of "grievous ambiguity" such that this Court cannot rely on the "text, structure, history, and purpose" of the Acts to resolve any "technically ambiguous" terms which would not "by itself make the rule of lenity applicable." *United States v. Lillard*, 935 F.3d 827, 829 (9th Cir. 2019); *Craigslist Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178, 1185 (N.D. Cal. 2013).

The cases cited by Defendant are distinguishable. For instance, Defendant cites to *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022) for the proposition that the rule of lenity precludes extending the language of an act to "technology that was not on the legislature's radar when it passed or amended those laws." Mot. at 29. However, *hiQ Labs, Inc.* did not grapple with applying a criminal law civilly to emergent technologies, instead citing the Ninth Circuit's application of the rule of lenity in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009) when analyzing the statutory term "without authorization," as had countless other cases applying the Computer Fraud and Abuse Act, many of which found the conduct applicable. 31 F.4th 1180, 1200 (9th Cir. 2022); *compare to Craigslist Inc*., 964 F. Supp. 2d at 1180 ("Under the plain language of the CFAA, defendant was 'without authorization' when it continued to pull data off of plaintiff's website after plaintiff revoked its authorization to access the website"). Here, Defendant does not ask the Court to interpret a genuinely ambiguous term that continues to be vague in the face of the statutory context.

The text, structure, history, and purpose of the State Wiretapping Acts have consistently reinforced the necessity to protect the privacy of person's communications. While session replay may not have been predictable when these Acts were passed, "[i]ncreasingly, courts must apply

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

old laws to new technology. In doing so, they can either acknowledge the unique features of modern technology, or . . . they can disregard these differences. Only the first approach allows courts to grapple with the legal issues generated when old law meets new tech." *Fin. Software Sys. v. Questrade, Inc.*, CV 18-742, 2018 WL 3141329, at *5 (E.D. Pa. June 27, 2018) (citing *Microsoft Corp. v. United States*, 130 Harv. L. Rev. 769, 769 (2016)). Accordingly, Defendant's manufactured ambiguities do not rise to the level in which the rule of lenity is appropriate to apply.

F. PLAINTIFFS HAVE SUFFICIENTLY PLED INTRUSION UPON SECLUSION

Plaintiffs have sufficiently pled claims for an invasion of privacy pursuant to the common law of Washington[5] (Count II), Pennsylvania[6] (Count IV), Illinois[7] (Count VII), and Missouri[8] (Count X), and more broadly, as guided by Restatement (Second) of Torts § 652B.

Microsoft's request to dismiss Plaintiffs' Intrusion upon Seclusion claims is based on five points: (1) Plaintiffs' visits to the Zillow website lack privacy and cannot reasonably expect privacy; (2) Microsoft's intrusion was not "unreasonable"; (3) Microsoft's intrusion is not "highly offensive"; (4) Plaintiffs did not allege lack of consent to use Clarity on Zillow's Website; and (5) Plaintiffs' Illinois intrusion upon seclusion claims fail to allege injury. However, Defendant is incorrect on each point as a matter of law. Plaintiffs adequately stated claims for relief, and the

[5] Washington State has adopted the Restatement of Torts Second Edition's understanding of invasion of privacy. *Peters v. Vinatieri*, 102 Wn. App. 641, 9 P.3d 909, 917 (Wash.Ct.App.2000) (a plaintiff must show that the defendant "intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns" and that "the intrusion would be highly offensive to a reasonable person.")

[6] "It is well established in Pennsylvania that a violation of the right of privacy is an actionable tort." *Tagouma v. Investigative Consultant Services, Inc.*, 4 A.3d 170, 174 (Pa. Super. 2010); To prevail on a claim for "intrusion upon seclusion," a plaintiff must show that (1) there was an intentional intrusion, (2) upon plaintiff's solitude or seclusion, or plaintiff's private affairs or concerns, and (3) the intrusion was substantial and highly offensive. *Id.*; *Reinhold v. County of York*, No. 1:11-CV-605, 2012 WL 4104793, at *18 n.23 (M.D.Pa.2012).

[7] "The elements required to prove intrusion upon seclusion are (1) an unauthorized intrusion or prying into the plaintiff's seclusion; (2) an intrusion that is highly offensive or objectionable to a reasonable person; (3) that the matter upon which the intrusion occurs is private; and (4) the intrusion causes anguish and suffering." *Jacobson v. CBS Broad., Inc.*, 386 Ill.Dec. 12, 19 N.E.3d 1165, 1180 (Ill. App. Ct. 2014). The essence of an intrusion upon seclusion is an "offensive prying into the private domain of another." *Lovgren v. Citizens First Nat'l Bank of Princeton*, 126 Ill. 2d 411, 417 (1989). Indeed, if the matter upon which the intrusion occurred is not private, there can be no cause of action for intrusion upon seclusion. *Jacobson*, 2014 IL App (1st) 132480, ¶ 47.

[8] To plead this claim under Missouri law, Plaintiffs must allege "(1) the existence of a secret and private subject matter; (2) a right in the plaintiff[ ] to keep that subject matter private; and (3) the obtainment by the defendant of information about that subject matter through unreasonable means." *Hester v. Barnett*, 723 S.W.2d 544, 562 (Mo. Ct. App. 1987); *see also, Durrell v. Tech Elecs., Inc.*, No. 4:16 CV 1367 CDP, 2016 WL 6696070, at *3 (E.D. Mo. Nov. 15, 2016).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

reliance on Terms of Use or proximate cause of injuries cannot be resolved at the pleading stage. *In re Facebook*, 956 F.3d at 601 ("At the pleading stage, all allegations of material fact are taken as true and construed in the light most favorable to the non-moving party."); *see also Dougherty v. City of Covina*, 654 F.3d 892, 897 (9th Cir. 2011); *Hewlett–Packard Co.*, 668 F.3d at 1140.

1. Plaintiffs have adequately alleged an objective, reasonable expectation of privacy in their Website Communications during visits to the Zillow Website and the use of Clarity is objectively unreasonable.

Plaintiffs have pleaded that Microsoft's use of Clarity to collect and record their electronic communications constitutes an intrusion upon seclusion. CAC ¶¶ 27–32, 94, 98. The Washington state constitution "clearly recognizes an individual's right to privacy with no express limitations." *State v. Young*, 123 Wash.2d 173, 180, 867 P.2d 593 (1994). The defendant's intrusion, whether ***physical or nonphysical***, must substantially interfere with the plaintiff's seclusion in a manner highly offensive or objectionable to a reasonable person. *Mark v. Seattle Times*, 96 Wash.2d 473, 497, 635 P.2d 1081 (1981).

First, Plaintiffs do have a reasonable expectation of privacy when inputting information into websites on their personal devices like computers or cell phones. CAC ¶¶ 1, 73–79, 92–93. Courts are increasingly recognizing that individuals may have a reasonable expectation of privacy in their web browsing history and private information divulged during internet activity. *United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008) (holding that URLs[9] reveal people's internet activity); *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 151 (3d Cir. 2015) (reasonable expectation of privacy in URL queries). A reasonable expectation of privacy can exist where a defendant gains access to data through electronic or covert means in violation of the law or social norms. *See In re Facebook*, 956 F.3d at 601–02. To illustrate, it is comparable to someone surreptitiously looking over your shoulder (and recording) while you browse the web, observing every mouse movement, click, and text input—certainly no one would consider that a "public matter." *Mark v. KING Broad. Co.*, 27 Wn. App. 344, 618 P.2d 512, 519

[9] *See In re Zynga Priv. Litig.*, 750 F.3d 1098, 1108–09 (9th Cir. 2014) ("Under some circumstances, a user's request to a search engine for specific information could constitute a communication such that divulging a URL containing that search term to a third party could amount to disclosure of the contents of a communication"). *See* CAC ¶¶ 20, 61.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

(1980) (an "invasion or intrusion must be of something which the general public would not be free to view.") Indeed, assuming *arguendo* that all Plaintiffs read the Terms of Use, Plaintiffs alleged they could not have known about the implementation of Session Replay or Microsoft Clarity,[10] as those terms are not explicitly anywhere on Zillow's Website, and Clarity is a third-party Plaintiffs know nothing about. CAC ¶ 28; *see also* Ex. 3[11] *but See Privacy Policy*, Zillow.com (Mar. 7, 2022) (attached as Exhibit A). Microsoft's Clarity technology remains largely unknown to the general public and is not readily accessible by the public. Plaintiffs have sufficiently demonstrated an objective, reasonable expectation of privacy at this stage.

Second, Microsoft argues that its intrusion on Plaintiffs' privacy was not "unreasonable" because Zillow's Terms of Use[12] disclosed "technology like Clarity." Mot. at 31. Microsoft's "reasonableness" argument is a premature question of fact that cannot be decided on a motion to dismiss as the Clarity program was never mentioned in the Terms of Use. *See supra* at 21. Plaintiffs and the Class members did not consent, in any form, to this intrusion. CAC ¶¶ 96, 106, 125, 133, 156, 163, 188, 210, 238, 266, 288. Plaintiffs, as any other reasonable person, would rationally expect that, outside of consent, activity on a personal device, no matter where the device is used, is private. CAC ¶¶ 16–17, 19, 21, 59, 79, 81-82, 86, 88, 95; *see also In re Facebook*, 956 F.3d at 604 n.7 ("[I]ndividuals maintain the expectation that entities will not be able to collect such broad swaths of personal information absent consent."). Moreover, while "consent by a plaintiff clearly negates the element of intentional intrusion upon the plaintiff's private affairs," the existence of consent is an issue of material fact. *Budsberg v. Trause*, 191 Wn. App. 1021 (2015) (where, on an appeal of dismissal on summary judgment, no genuine issue of material fact existed to dispute consent). Thus, Microsoft's recordings of Plaintiffs on their personal devices, without explicit written or published consent, is unreasonable.

---

[10] Clarity allows Zillow to select specific elements and content to mask or unmask, and specific elements may vary based on the Configuration selected. CAC ¶¶ 37, 64. Plaintiffs need not allege which specific masking setting was employed, and such reasonableness is a question of fact that cannot be decided at the pleading stage. *In re Facebook*, 956 F.3d at 601.

[11] Ex. 3 shows Zillow's Privacy Policy to be effective January 2023. This is not consistent with the Privacy Policy that was in effect during Plaintiffs' experiences, which began as early as 2010 and prior to 2022. CAC ¶¶ 71–79.

[12] *See infra* at 25 (discussing browsewrap and consent in more detail).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

2. **Microsoft's Tracking and Recording without Consent is Highly Offensive**

The means by which Microsoft tracked and recorded Plaintiffs' website interactions was highly offensive and invasive because Zillow's website users would not expect or detect an invasion beginning immediately on a routine visit to the website. "[T]he highly offensive analysis focuses on the degree to which the intrusion is unacceptable as a matter of public policy." *In re Facebook*, 956 F.3d at 606. The "highly offensive to a reasonable person" element requires a "holistic consideration of factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder's motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive." *Id.* at 606. The analysis also "focuses on the degree to which the intrusion is unacceptable as a matter of public policy." *Id.* Whether something is highly offensive is a matter subject to community standards and necessitates a jury's determination as it is a triable issue of fact. *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1080 (N.D. Cal. 2016).[13]

The conduct is highly offensive when considering Plaintiffs' and Class members' expectation that website providers obtain consent before collecting and sharing consumer data. CAC ¶¶ 28–30. Microsoft attempts to soften its conduct by stating that internet tracking is "commonplace," Mot. at 32, but this misses the mark. What is important is "*how* [defendant] accomplished its tracking." *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 292 (3d Cir. 2016) (finding defendant's behavior to be highly offensive); *see also In re Google*, 806 F.3d at 151 (finding defendant's conduct "highly offensive" where the defendant's conduct of acquiring URL queries was surreptitious). The act of concealing oneself for purposes of surreptitiously wiretapping, combined with the unfiltered, non-stop recording in real-time of each and every visit and interaction with Zillow's website without any semblance of explicit consent[14] *is* highly offensive conduct.

[13] The rationale presented in *In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968 (N.D. Cal. 2014) is unhelpful because that court's failed to explain how Google's practices aligned with prevailing community privacy norms at the time of the ruling. *Opperman*, 205 F. Supp. 3d at 1079.

[14] "If voluntary consent is present, a defendant's conduct will rarely be deemed 'highly offensive to a reasonable person' so as to justify tort liability." *Hill v. Nat'l Collegiate Athletic Assn.*, 865 P.2d 633, 648 (1994).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Microsoft's reliance on *Boring v. Google Inc.*, 362 F. App'x 273 (3d Cir. 2010), regarding the invasion claim over Google Maps's Street View photos of plaintiffs' residence is misplaced, as it contradicts the principle outlined in *King Broadcasting Co.*, 618 P.2d at 519, which emphasizes that invasion must involve something not freely visible to the public.

Microsoft misstates the decision in *Nickelodeon*. 827 F.3d 262. There, the court found that plaintiff alleged an intrusion claim against defendant Viacom.[15] Any deceit or disregard can be considered "conduct highly offensive or an egregious breach of social norms"; without "legal or personal permission," Viacom could not collect or disclose personal information. *Id*. at 293. Likewise, here, Plaintiffs never provided any legal or personal permission for Microsoft to record their website communications, as such recordings begin immediately without any option to first provide consent. CAC ¶¶ 96–99.

Microsoft's reliance on *Hammerling v. Google* is also misplaced as that case involved issues of "usage and engagement" data, such as the average number of days users were active on specific apps and their total time spent on non-Google apps. 615 F. Supp. 3d 1069, 1078 (N.D. Cal. 2022). Importantly, there, plaintiffs did not claim that Google could read specific user-inputted text (content). *Id*. at 1093. Thus, the data collected in *Hammerling* differs significantly from the data in the current matter, as Plaintiffs have alleged that text inputted by a user can be read and recorded. *See* CAC ¶¶ 34, 37, 39, 43, 85–86, 89, 92, 95. Thus, at this stage, Plaintiffs sufficiently plead the "highly offensive" prong.

3. Microsoft was "substantially certain" that it lacked Plaintiffs' consent, as the intrusion began immediately, leaving no opportunity to seek consent beforehand.

Plaintiffs have alleged sufficient facts that show the intrusion occurred immediately once they entered the website, as the monitoring, collecting, and recording "begins *immediately* upon arriving at Zillow's Website." *See* CAC ¶¶ 96–99. Plaintiffs were never provided an opportunity to consent. *See supra*, at 7. At most, Zillow's Terms of Use and privacy statement constitute

[15] Here, the court stated that defendant Google's use of "third-party *cookies*" was not "sufficiently offensive" as to claims against Google only.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

unenforceable browsewrap. "[W]here, as here, there is no evidence that the website user had actual knowledge of the agreement, the validity of the browsewrap agreement turns on whether the website puts a reasonably prudent user on inquiry notice of the terms of the contract. Whether a user has inquiry notice of a browsewrap agreement, in turn, depends on the design and content of the website and the agreement's webpage. Where the link to a website's terms of use is buried at the bottom of the page or tucked away in obscure corners of the website where users are unlikely to see it, courts have refused to enforce the browsewrap agreement." *Barnes & Noble Inc*., 763 F.3d at 1177; *see also, Nicosia v. Amazon.com, Inc.*, 834 F.3d 220, 233 (2d Cir. 2016); *Foster v. Walmart, Inc.*, 15 F.4th 860, 865 (8th Cir. 2021). Thus, there are ample facts indicating the Microsoft was substantially certain that plaintiffs had not provided adequate consent, which further supports Plaintiffs' claims.

4. Plaintiffs have alleged a sufficient actual injury, pursuant to Illinois Law.

In *TransUnion, LLC v. Ramirez* (2021), the Supreme Court held that various intangible harms, such as reputational harms, disclosure of private information, and intrusion upon seclusion, can be considered concrete. 141 S. Ct. 2190, 2200 (2021). In *Schmidt v. Ameritech Illinois* (2002), the court found that the record did not establish the intrusion as the proximate cause of the plaintiffs' suffering. 768 N.E.2d 303, 31 (2002). Here, the Illinois Plaintiffs have sufficiently alleged that the intrusion was the proximate cause of their "mental anguish" and "suffering." CAC, ¶ 214.

IV. THE COURT SHOULD STRIKE MICROSOFT'S PRIVACY POLICY

Plaintiffs request the Court strike Microsoft's Exhibit 3 to its Motion to Dismiss purporting to attach Zillow's applicable Privacy Policy and, also, Microsoft's references to that policy in its Motion. A motion to strike is appropriate where the material at issue is "irrelevant" and "has no possible bearing on the litigation's subject matter." *Adamson v. Pierce County*, 2023 WL 4296383, at *2 (W.D. Wash. June 30, 2023). Here, Microsoft extensively relies on the Privacy Policy put in place after the litigation began to claim Plaintiffs previously consented to the use of Clarity and lacked a reasonable expectation of privacy. Mot. at 4, 12–13, 15, 31, 33.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Microsoft's claim should be rejected, and the Privacy Policy stricken as an exhibit. The Privacy Policy Microsoft relies on was not enacted until ***after*** Plaintiffs filed their initial actions and, thus, is irrelevant to the claims or defenses in this case. Each Plaintiff filed his or her initial complaint between September and December 2022, which was later consolidated here. *See* ECF No. 33 (listing related actions and granting a joint stipulation to consolidate the actions before the Court). However, the Privacy Policy Microsoft attaches has an **"[e]ffective [d]ate"** of "January 2023." *See* Mot. Ex. 3 at 1.

The Privacy Policy Microsoft relies on was, thus, not in effect when Plaintiffs allege they were surreptitiously recorded. Plaintiffs could not have viewed the policy or relied on it when navigating Zillow's website. Contrary to Microsoft's claims, the Privacy Policy in place beforehand excluded any information about the use of session replay technology. *See* Ex. A..[16] Indeed, Microsoft extensively quotes the new Privacy Policy to assert Plaintiffs consented to the use of session replay technology. Mot. at 12. However, the provisions it quotes do not exist in the policy in place at the time Plaintiffs were navigating Zillow's website and their information was improperly acquired by Clarity.

Consequently, the Privacy Policy Microsoft attaches to its Motion has no bearing on the issues of consent or expectation of privacy or any other issue. The Court should strike Exhibit 3 and Microsoft's references to that Exhibit in its Motion to Dismiss.

Dated: July 31, 2023

Respectfully submitted,

TOUSLEY BRAIN STEPHENS PLLC

s/ Kim D. Stephens, P.S.
Kim D. Stephens, P.S., WSBA #11984
kstephens@tousley.com
s/ Jason T. Dennett
Jason T. Dennett, WSBA #30686
jdennett@tousley.com

[16] There was no update to the Privacy Policy between March 7, 2022 and January 2023, therefore the fact applicable Privacy Policy is attached as Exhibit A. *See, Zillow Privacy Policy as archived on Waybachmachine.com*, https://web.archive.org/web/20220801210928/https://www.zillowgroup.com/zg-privacy-policy/

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

s/ Kaleigh N. Boyd
Kaleigh N. Boyd, WSBA #52684
kboyd@tousley.com
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
Telephone: (206) 682-5600
Fax: (206) 682-2992

Gary F. Lynch (*pro hac vice*)
Kelly K. Iverson (*pro hac vice*)
Jamisen A. Etzel (*pro hac vice*)
Elizabeth Pollock-Avery (*pro hac vice*)
Nicholas A. Colella (*pro hac vice*)
Patrick D. Donathen (*pro hac vice*)
LYNCH CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, Pennsylvania 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
gary@lcllp.com
kelly@lcllp.com
jamisen@lcllp.com
elizabeth@lcllp.com
nickc@lcllp.com
patrick@lcllp.com

Joseph P. Guglielmo, (*pro hac vice*)
Carey Alexander (*pro hac vice*)
Ethan S. Binder (*pro hac vice*)
SCOTT+SCOTT ATTORNEYS
AT LAW LLP
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169
Telephone: (212) 223-6444
Facsimile: (212) 223-6334
jguglielmo@scott-scott.com
calexander@scott-scott.com
ebinder@scott-scott.com

E. Kirk Wood (*pro hac vice* forthcoming)
Sharika Robinson (*pro hac vice* forthcoming)
Marcela Jenkins (*pro hac vice* forthcoming)
WOOD LAW FIRM, LLC
P. O. Box 382434

Birmingham, AL 35238-2434
Telephone: (205) 908-4906
kirk@woodlawfirmllc.com
marcelaj@blalocklegal.com

Tiffany Marko Yiatras (*pro hac vice* forthcoming)
CONSUMER PROTECTION LEGAL, LLC
308 Hutchinson Road
Ellisville, Missouri 63011-2029
Tele: (314) 541-0317
Email:
tiffany@consumerprotectionelegal.com

Bryan L. Bleichner (*pro hac vice* forthcoming)
CHESTNUT CAMBRONNE PA
100 Washington Avenue S, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com

Kate M. Baxter-Kauf (*pro hac vice* forthcoming)
Karen Hanson Riebel (*pro hac vice* forthcoming)
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
kmbaxter-kauf@locklaw.com
khriebel@locklaw.com

Joshua B. Swigart (*pro hac vice* forthcoming)
SWIGART LAW GROUP, APC
2221 Camino del Rio S, Ste 308
San Diego, CA 92108
Telephone: (866) 219-3343
Josh@SwigartLawGroup.com

Daniel G. Shay (*pro hac vice* forthcoming)
LAW OFFICE OF DANIEL G. SHAY
2221 Camino del Rio S, Ste 308
San Diego, CA 92108
Telephone: (619) 222-7429

DanielShay@TCPAFDCPA.com

Ari H. Marcus (*pro hac vice*)
Joseph H. Kanee (*pro hac vice* forthcoming)
MARCUS ZELMAN LLC
701 Cookman Avenue, Suite 300
Asbury Park, New Jersey 07712
Telephone: (732) 695-3282
Facsimile: (732) 298-6256
Ari@marcuszelman.com
joseph@marcuszelman.com

Brian C. Gudmundson (*pro hac vice*)
Rachel K. Tack (*pro hac vice*)
ZIMMERMAN REED LLP
1100 IDS Center
80 South 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
Facsimile: (612) 341-0844
brian.gudmundson@zimmreed.com
rachel.tack@zimmreed.com

Jonathan M. Jagher
FREED KANNER LONDON
& MILLEN LLC
923 Fayette Street
Conshohocken, Pennsylvania 19428
Telephone: (610) 234-6486
jjagher@fklmlaw.com

Douglas A. Millen
Michael E. Moskovitz
FREED KANNER LONDON
& MILLEN LLC
2201 Waukegan Road, Ste. 130
Bannockburn, IL 60015
Telephone: (224) 632-4500
dmillen@fklmlaw.com
mmoskovitz@fklmlaw.com

Attorneys for Plaintiffs and the Putative Class

CERTIFICATION

I certify that this memorandum contains 9,938 words, in compliance with the Local Civil Rules.

s/ Kim D. Stephens, P.S.
Kim D. Stephens, P.S., WSBA #11984

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992